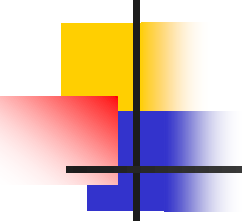




Data/Information Security Breach Response

May 17, 2012

Prepared by:
The Risk Management & Tort Defense Division



Most state, federal, and foreign breach notice laws require state agencies to notify individuals who are affected by a breach.



What is a Breach?

“Breach” means unauthorized acquisition of data that:

- (a) materially compromises the security, confidentiality, or integrity of the personal information maintained by a state agency or by a third party on behalf of the state agency; and
- (b) causes or is reasonably believed to cause loss or injury to a person.



“Personal Information”

“Personal information” means

(a) first name or first initial and last name in combination with any one or more of the following data elements when the name and the data elements are not encrypted:

(i) a social security number or tax identification number;

(ii) a driver's license number, an identification number issued pursuant to 61-12-501, a tribal identification number or enrollment number, or a similar identification number issued by any state, the District of Columbia, the Commonwealth of Puerto Rico, Guam, the Virgin Islands, or American Samoa; or

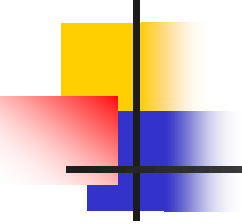
(iii) an account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account.

(b) The term does not include publicly available information that is lawfully made available to the general public from federal, state, local, or tribal government records.

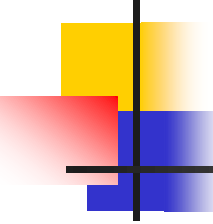


Report Breaches to RMTD Immediately

- Upon discovery or notification of a potential breach of personal information, the state agency that maintains the personal information shall notify the Risk Management & Tort Defense Division immediately.
- If a loss occurs during normal business hours you may reach RMTD claims staff at their phone extensions <http://rmtd.mt.gov/aboutus/organizationstaff.mcpix> or call (406)444-2421. In the event of an emergency, after normal business hours call (406)444-2421 and press 1. for Gordon Amsbaugh, 2. for Jennie YOUNKIN, or 3. for Brett Dahl. Your phone call will then be transferred to a live person. Note: Do not call after hours unless there is a true emergency, but please report the claim within 24 hours.
- The immediate supervisor must assure that the “Report of Incident” form <http://rmtd.mt.gov/claims/agenciesreportclaims.mcpix> is accurately completed, signed, and sent to RMTD within 2 business days.



Failure to properly notify individuals affected by a breach may result in identity theft, damage to state agencies' reputation, and regulatory fines and penalties from state and federal agencies.



RMTD participates in a national cyber/data information insurance exchange that offers basic insurance coverage to comply with state and federal law. The insurance provides coverage including, but not limited to:

- Privacy notification
- Credit monitoring
- Forensics
- Other services



Insurances does NOT cover everything

- You pay 20% (i.e. co-pay).
- Losses not covered by insurance may be the responsibility of your agency.
- The goal is to **PREVENT BREACHES!**



Prevent Breaches

- IT security controls
- Computer password controls
- Portable laptop and electronic device controls
- Management controls regarding access, use, and distribution of personal information



This is a Big Deal!

Utah

During routine server maintenance personal information of over 800,000 individuals was disclosed. The cost to notify individuals and provide credit monitoring services is estimated at \$12,000,000.



This is a Big Deal (cont'd)

Montana

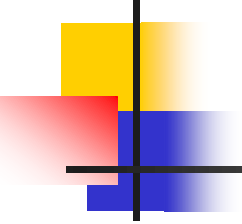
The Financial Industry Regulatory Authority fined D.A. Davidson & Co. in Great Falls \$375,000 for failing to protect confidential customer information from hackers despite a recommendation from security consultants to install an intrusion detection system.



More Examples

Texas

The Texas Comptroller's Office discovered that unencrypted data from the Teacher's Retirement System had been posted on the state's public servers for more than a year exposing 3.5 million individuals to potential identity theft. The information contained names, addresses, social security numbers, and other personally identifiable information. Regulatory fines are pending. A class action lawsuit seeking a \$1,000 penalty for each individual has been filed.



More Examples (cont'd)

Washington D.C.

An external hard drive containing one terabyte of data from the Clinton Administration was stolen from the National Archives and Records Administration (NARA). The information included more than 250,000 names, addresses, and social security numbers. This breach will cost NARA an estimated \$5 million to notify affected parties, provide credit monitoring services, and pay potential regulatory fines/penalties.